AI Risk Repository Chatbot: User Feedback & Improvement Plan

# Executive Summary

The AI Risk Repository Chatbot has been successfully integrated into airisk.mit.edu via Webflow embedding. To optimize user experience and ensure the tool meets researcher and practitioner needs, we propose a structured feedback gathering initiative with the FutureTech team and adjacent stakeholders. This document outlines our methodology for collecting actionable insights and implementing data-driven improvements.

# Current State & Challenge

## What We Have

* Fully functional chatbot embedded in airisk.mit.edu
* Direct navigation from main site "Chatbot" tab to /chat interface
* Working query processing for 1,612 AI risks across 7 domains
* Citation system linking to source documents

## The Challenge

As developers, we have "curse of knowledge" - we understand the system's capabilities and limitations intimately. We need fresh perspectives to understand:

* What new users expect vs. what they experience
* Whether the current interface supports user goals effectively
* What barriers prevent successful task completion

# Proposed Feedback Methodology

## Phase 1: User Research (Weeks 1-2)

### A. Structured User Testing Sessions

**Participants:** 10-12 people (45 minutes each)

* 4 FutureTech team members
* 3 AI/ML researchers (external to MIT)
* 3 policy/governance professionals
* 2 graduate students in relevant fields

**Test Tasks:**

1. 1. Find information about AI privacy risks
2. 2. Understand how the repository categorizes risks
3. 3. Explore employment impacts of AI
4. 4. Locate specific statistics about AI safety

**What We'll Measure:**

* Task completion rates
* Time to first meaningful interaction
* Points of confusion or abandonment
* Understanding of system capabilities

### B. Quick Intercept Surveys

Deploy a brief 3-question survey after users interact with the chatbot:

1. 1. Did you find what you were looking for? (Yes/Partially/No)
2. 2. What would make this tool more useful? (open text)
3. 3. How likely are you to recommend this? (1-10 scale)

## Phase 2: Analysis & Prioritization (Week 3)

* Synthesize findings into key themes
* Create priority matrix (High/Low Impact vs. Easy/Hard Implementation)
* Develop specific design recommendations

## Phase 3: Implementation (Weeks 4-6)

* Address quick wins immediately
* Design solutions for major issues
* A/B test significant changes

# Key Questions to Answer

## 1. Onboarding & First Impressions

* Should users see a welcome page before the chat interface?
* Do users understand what the chatbot can/cannot do?
* Are example queries or guided options needed?

## 2. Interface Design Decisions

**Current:** Full-page embedded chat via iframe

**Alternative A:** Floating chat widget that expands

**Alternative B:** Split interface with browse + chat options

**Alternative C:** Progressive disclosure starting with search bar

## 3. User Intent & Success

* What are users actually trying to accomplish?
* Can they complete their intended tasks?
* What queries fail most often?

## 4. Trust & Understanding

* Do users trust the responses?
* Is the MIT affiliation/credibility clear?
* Do users understand citations and use them?

# Specific Feedback Areas

## High Priority

1. **Entry Point:** Is direct navigation to /chat optimal, or do users need context?

2. **Capability Communication:** How can we better convey what the system knows?

3. **Error Handling:** What happens when users ask out-of-scope questions?

4. **Mobile Experience:** How well does the iframe embed work on phones/tablets?

## Medium Priority

1. Query suggestions or autocomplete

2. Conversation history/export features

3. Integration with main repository browse function

4. Visual indicators of processing/loading states

## Future Considerations

1. Personalization for different user types

2. Multi-language support expansion

3. API access for programmatic queries

# Timeline & Resources

## Week 1-2: Data Collection

* Recruit participants
* Conduct user sessions
* Deploy analytics and surveys

## Week 3: Analysis

* Synthesize findings
* Create priority recommendations
* Design mockups for major changes

## Week 4-6: Implementation

* Fix identified pain points
* Implement high-priority features
* Deploy A/B tests

## Required Resources

* 10-12 hours of user testing time
* 1-2 team members to conduct sessions
* Development time for implementing changes

# Success Metrics & Expected Outcomes

## Key Performance Indicators

1. **Engagement Rate:** >60% of visitors ask at least one question

2. **Success Rate:** >75% of queries answered satisfactorily

3. **Return Rate:** >30% return within one week

4. **Net Promoter Score:** >7/10 average

## Deliverables

1. **Feedback Report** with synthesized findings and recommendations

2. **Priority Roadmap** for UI/UX improvements

3. **Updated Interface** based on user feedback

4. **Best Practices Guide** for future iterations

# Next Steps

1. **Approval** of this feedback plan

2. **Recruitment** of test participants from FutureTech and adjacent teams

3. **Scheduling** of user testing sessions

4. **Implementation** of quick analytics to establish baselines

# Questions for Discussion

1. Are there specific user groups we should prioritize?

2. What aspects of the current implementation are non-negotiable?

3. What is our budget/timeline for implementing changes?

4. Should we coordinate with the main airisk.mit.edu redesign efforts?

*Contact: David Turturean | Last Updated: November 2024*